We claim:

1. A method of producing an executable instance of a software application in a secure hardware adjunct where secure processing is performed, the method comprising the steps of:

providing a non-executable form of a software application to the secure hardware adjunct,

providing sensitive functions to the secure hardware adjunct,

transforming the non-executable form of the software application into an executable form of the software application in the secure hardware adjunct;

integrating the sensitive functions with the executable form of the software application in the secure hardware adjunct to produce an executable instance of the software application; and

outputting the executable instance of the software application to a digital appliance.

2. The method of claim 1 wherein the sensitive functions comprise one or more of the following:

i. a digital rights management algorithm;

ii. a user authentication algorithm;

iii. a user contract determination algorithm;

iv. a cryptographic key request and download algorithm; and

v. an algorithm for scanning the digital appliance for appliance-specific identifiers.

Species

3. The method of claim 1 further including the steps of:

locating the non-executable form of the software application and the sensitive functions on an Internet server; and

downloading the non-executable form of the software application and the sensitive functions from the Internet server.

4. The method of claim 1 wherein the secure hardware adjunct is implemented by one of the following:

i. a secure integrated circuit on a motherboard of the digital appliance;

ii. a secure integrated circuit on an expansion board of the digital appliance;

iii. an external device connected to the digital appliance through an external port;

iv. a smart card and smart card reader; or

v. a component of a wireless Internet-enabled handheld device.

5. The method of claim 1 further including the step of: following the transforming step, varying the positioning of binary instructions of the executable form of the software application in the secure hardware adjunct.

6. The method of claim 1 wherein the step of transforming includes the step of using a private decryption key stored in the secure hardware adjunct to decrypt the non-executable form of the software application.

7. The method of claim 1 further including the step of executing the executable instance of the software application in the digital appliance immediately upon completion of the outputting step.

8. The method of claim 1 further including the steps of:

inspecting the digital appliance for environmental data;

providing the environmental data to the secure hardware adjunct.

9. The method of claim 8 further including the step of:

embedding the environmental data in the executable instance of the software application, the environmental data functioning upon execution of the software application to restrict execution to the digital appliance.

10. The method of claim 8 further including the steps of:

prior to the integrating step, using the environmental data to select, from among the provided sensitive functions, a subset of sensitive functions to be integrated into the executable form of the software application.

11. The method of claim 8 further including the steps of:

following the outputting step, re-inspecting the digital appliance for environmental data;

executing the executable instance of the software application only if the environmental data provided to the secure hardware adjunct matches the environmental data located during the re-inspecting step.

12. The method of claim 8 wherein the environmental data consists of information about one or more of the following:

i. the digital appliance executing the executable instance of the software application;

ii. a user;

iii. the secure hardware adjunct; and

iv. network accessible resources.

13. The method of claim 1 further including the steps of:
locating environmental data on an Internet server;
authenticating the environmental data;
encrypting the environmental data;
downloading the environmental data from the Internet server to the secure hardware adjunct; and
decrypting the environmental data in the secure hardware adjunct.

14. The method of claim 8 wherein the secure hardware adjunct is a bus master, capable of inspecting the digital appliance independent of any hardware or software contained in the digital appliance.

15. The method of claim 8 wherein the inspecting and providing steps are performed under the control of an auxiliary external software program.

16. The method of claim 1 further including the step of inspecting the secure hardware adjunct for environmental data.

17. The method of claim 1 wherein the step of providing a non-executable form of a software application to the secure hardware adjunct includes the following steps:
embedding a private decryption key in the secure hardware adjunct;
encrypting the software application with a public encryption key corresponding to the private decryption key to produce a non-executable form of the software application;

downloading the non-executable form of the software application from an Internet server to the secure hardware adjunct.

18. The method of claim 1 further including the steps of:

executing the executable instance of the software application in the digital appliance;

verifying the status of the secure hardware adjunct;

if the status of the secure hardware adjunct is changed, then ceasing the execution of the executable instance of the software application.

19. The method of claim 18 further including the step of:

passing control over the executable instance of the software application to an integration framework software process, so that said process might provide recovery action beyond simply stopping the application.

20. The method of claim 1 further including the steps of:

scanning the digital appliance for identification data;

providing the identification data to the secure hardware adjunct;

integrating the identification data with the executable form of the software application;

and wherein the outputted executable instance of the software application further incorporates the identification data.

21. The method of claim 1 wherein the step of integrating includes the following:

selecting, from among the provided sensitive functions, a subset of sensitive functions to be integrated into the executable form of the software application.

22. The method of claim 1 wherein the non-executable form of the software application cannot be rendered executable without the integration of the sensitive functions.

23. The method of claim 1 further including the steps of:

requesting the entry of a personal identification number; and

executing the executable instance of the software application only if the entered personal identification number matches a personal identification number integrated into the executable instance of the software application.

24. The method of claim 1 further including the steps of:

providing encrypted data files associated with the non-executable form of the software application to the secure hardware adjunct;

decrypting the encrypted data files in the secure hardware adjunct.

25. The method of claim 1 further including the step of:

authorizing the rights of a user to access the executable instance of the software application and only proceeding to the transforming, binding and outputting steps if the user's rights have been authorized.

26. The method of claim 26 wherein the step of authorizing includes the steps of:

embedding the secure hardware adjunct with a reserve of electronic cash;

initiating an interaction with a banking server; and

deducting a payment from the reserve of electronic cash.

27. A secure hardware adjunct comprising:

a processor where secure processing can be performed,

read only memory connected to said processor;

random access memory connected to said processor;

input and output paths for communication between the processor and a digital appliance;

a secure housing covering the processor, the read only memory and the random access memory, the secure housing being resistant to tampering and observation of data and algorithms in the processor, the read only memory and the random access memory;

the processor, upon being provided with a non-executable form of a software application and sensitive functions on the input path, transforms the non-executable form of the software application into an executable form of the software application; integrates the sensitive functions with the executable form of the software application to produce an executable instance of the software application; and outputs on the output path the executable instance of the software application to the digital appliance.

28. The secure hardware adjunct of claim 27 wherein said processor is connected to a smart card reader.

29. The secure hardware adjunct of claim 27 wherein said processor comprises part of an integrated circuit on an expansion board of the digital appliance.

30. The secure hardware adjunct of claim 27 wherein the sensitive functions comprise one or more of the following:

i. a digital rights management algorithm;

ii. a user authentication algorithm;

iii. a user contract determination algorithm;

iv. a cryptographic key request and download algorithm; and

v. an algorithm for scanning the digital appliance for appliance-specific identifiers.

31. Computer readable medium storing processor executable instructions for use in producing an executable instance of a software application in a secure hardware adjunct where secure processing is performed, the secure hardware adjunct being provided with a non-executable form of a software application and sensitive functions, the processor executable instructions when loaded at a processor in the secure hardware adjunct adapt said processor to:

transform the non-executable form of the software application into an executable form of the software application;

integrate the sensitive functions with the executable form of the software application to produce an executable instance of the software application; and

output the executable instance of the software application to the digital appliance.

32. The computer readable medium of claim 31 wherein the secure hardware adjunct is implemented by one of the following:

i. a secure integrated circuit on a motherboard of the digital appliance;

ii. a secure integrated circuit on an expansion board of the digital appliance;

iii. an external device connected to the digital appliance through an external port;

iv. a smart card and smart card reader; or

v. a component of a wireless Internet-enabled handheld device.

33. The computer readable medium of claim 31 wherein the sensitive functions comprise one or more of the following:

i. a digital rights management algorithm;

ii. a user authentication algorithm;

iii. a user contract determination algorithm;

iv. a cryptographic key request and download algorithm; and

v. an algorithm for scanning the digital appliance for appliance-specific identifiers.